Protected Core Networking – Concepts & Challenges

Mr Roland SCHUTZ
160, Boulevard de Valmy
BP82 – 92704 Colombes Cedex
FRANCE

Roland.schutz@fr.thalesgroup.com

ABSTRACT

The objective of this paper is to address the transformation that is required for introduction of the PCN concepts in the developments of future static and deployed infrastructures.

The paper will discuss this transformation that will in a first step present how these concepts shall be applied in the deployment of a coalition, then analyse the impact of this transformation on the service value chain. The objective is to show how the end-user service will be delivered based on services provided by the networking layers of the architecture, and to propose an Architecture Framework that needs to be applied in the context of PCN compliant networks.

The paper will also discuss the policies that shall be developed in order to guarantee interoperability of the PCSs in the PCN and the implementation of the concepts, as it is admitted that all the capabilities defined by the PCN RTO Working Group will not be implemented in the early steps of the deployment. These policies address the routing, QoS and security issues; they define the homogeneity of the behaviour of the PCSs at the interoperability points.

The presentation will also deepen the interfaces of the PCSs with the Bearer Networks and show how the undergoing transformation (to Ethernet) of the Bearer Network will support the deployment of the PCN concept.

INTRODUCTION

An early adoption of the PCN concepts by the Nations and by NATO requires further definition on how these concepts will be implemented and deployed in the context of a coalition. These further definitions have to address the general policies to be agreed by all the stakeholders that will adopt the transformation required by these concepts.

The RTO PCN working Group produced the "Requirements for a Protected Core Networking (PCN) Interoperability Specification (ISpec)". This initial report addresses the objectives and capabilities to be reached, the PCN concept that will allow a global share of the deployed infrastructure, and the main interfaces (PCN-1 dedicated to interoperability between the PCSs and PCN-2 dedicated to the PCN user access).

Other policies have been issued by NATO in the field of Quality of Service (QENI, IP QoS Standardisation for the NII, SLA management) and Security (INFOSEC Technical and Implementations Directives). These directives will apply when implementing the PCN concept for the creation of a federation of networks. They will need to be completed with additional policies describing a shared behaviour and a common understanding of the user and interoperability services provided by the PCN.

The main objectives of this paper is to deepen the implementation of the PCN, and discuss, through an example of a coalition network involving NATO and several NATO Nations, how the PCN concepts

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
NOV 2010	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Protected Core Networking Concepts & Challenges	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Thales Group 160, Boulevard de Valmy BP82 92704 Colombes Cedex FRANCE**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADA564697. Information Assurance and Cyber Defence (Assurance de l'information et cyberdefense). RTO-MP-IST-091

14. ABSTRACT
The objective of this paper is to address the transformation that is required for introduction of the PCN concepts in the developments of future static and deployed infrastructures. The paper will discuss this transformation that will in a first step present how these concepts shall be applied in the deployment of a coalition, then analyse the impact of this transformation on the service value chain. The objective is to show how the end-user service will be delivered based on services provided by the networking layers of the architecture, and to propose an Architecture Framework that needs to be applied in the context of PCN compliant networks. The paper will also discuss the policies that shall be developed in order to guarantee interoperability of the PCSs in the PCN and the implementation of the concepts, as it is admitted that all the capabilities defined by the PCN RTO Working Group will not be implemented in the early steps of the deployment. These policies address the routing, QoS and security issues; they define the homogeneity of the behaviour of the PCSs at the interoperability points.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**10**	

could be applied, based on the capabilities and capacities provided by the underlying Bearer Networks (operator sub-network, Satellite sub-network, LOS sub-network, and Radio sub-network).

APPLICATION OF THE PCN CONCEPT TO A COALITION NETWORK

The scenario in support of this paper consists of the deployment of NATO Forces with the support of Forces deployed by three Nations, involving a terrestrial and a maritime component. The maritime Component is represented by the fleet of one of the coalition Nation. The terrestrial forces are composed of the Joint Task Force hosting the LCC, and ACC under NATO command, and the terrestrial deployment of each of the Nations.

From an operational point of view, the following figure shows the characteristics of the deployment. In order to ensure the mission the coalition will require the capability to exchange Information:

- Between NATO and Nations' Static Head Quarters, relative to the Coordination and Consultation processes
- Between the Static Headquarters and the Deployed Head Quarters of a same organisation
- Between the Deployed Head Quarters and the Deployed Operational Bases (DOB), and also in-between the DOBs ((Brigade, Battalion, and Companies)

The Communication capabilities needed for the mission are Voice and VTC, File transfer, Messaging, Remote Portal Access, Interactive Messaging, Media Steaming and Video.

The links between the operational bases represents the capacity required between the bases for the mission.

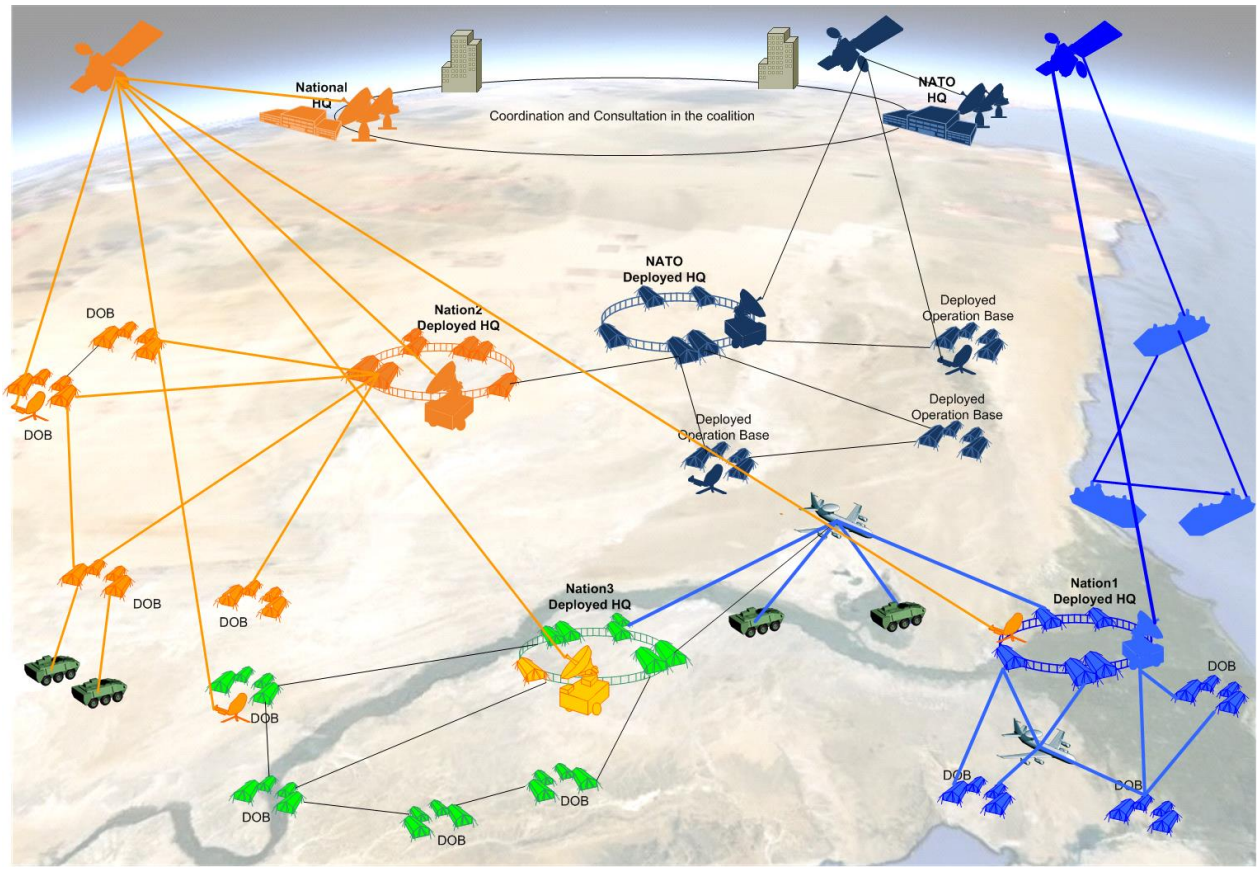

Figure 1 - Operational View

The capacity required for the interconnection of the different Operational Nodes (Deployed or in the Reachback) will be provided by bearer sub-networks.

Let's consider that the access capabilities provided by the bearer sub-networks are based on a physical Ethernet Interface providing a Virtual Private Wire Service (VPWS), or a Virtual Private LAN Service (VPLS). These services have been specified by the Metro Ethernet Forum (MEF), and are now available as services provided by the Public Telecom Operators.

In the military of the shelf (MOTS) solutions, early implementations of these services defined by the MEF are now available for integration and deployment, as precise examples:

- The Thales 21e satellite modem solution provides a satellite point to point mesh capability through its Ethernet interface specified according to MEF VPWS services. In addition to this networking capability the modem takes into account advanced protection mechanisms of the links carried over the satellite.
- The Thales Line Of Sight (LOS) solution provides interconnection capabilities based on an Ethernet interface specified according to MEF VPWS Services.
- Undergoing developments in Software Defined Radio (SDR) solutions will also provide such capabilities (UHF radios for interconnection in the Maritime Field)

These solutions already integrate capabilities for management of 802.1Q defined Class of Services; and future evolution will take into account VPLS capabilities. NATO NII Communication Reference

Architecture [NCRA] named "B_{REF}" the interface with the bearer sub-networks. The same identification is used in the following diagrams for this interface.

In the present approach the bearer sub-networks should not be considered as PCSs. These networks are only the bearers of the interfaces (PCN-1, PCN-2) defined by the PCN RTO Working Group, and they will provide the capacity for interconnection of the Protected Core Segments, and for interconnection of the PCS Nodes in point to point (Trunks) and also in a point to multipoint mode.

The organisation presented below, shows the possibility to integrate, in a same PCS, Non protected Bearer solutions provided by Public Telecom Operators, and protected solutions based on hardened modems integrating protection mechanisms. In case of non protected bearer solution, the PCS node will need to handle the protection mechanisms before sending the Ethernet frames over the un-trusted bearer network.

This transformation from PDH/SDH services to Ethernet Frame based Services (VPWS, VPLS) requires management of transport Class of Services in conformance with the functionalities specified by the standardisation bodies (IETF, MEF, IEEE). The bearer sub-networks need to implement following Class of Services:

- Real Time COS for transport of Voice, Circuit Emulation flows, and applications expecting very low latency
- Near Real Time COS for transport of VTC and Video Streaming flows, and also for specific Data application
- Interactive COS for transport of flows requiring interactivity (Database Browsing, Web Browsing, Chatting, and high Precedence Messaging)
- Bulk transfer COS dedicated to File Transfer and low Precedence Messaging
- Best Effort for low precedence activities (Internet access, etc)

The services provided by the bearer network need to be provisioned in order to make sure that the Protected Core Segments (PCSs) connecting the users via the PCN-2 interface, and interconnecting with adjacent PCSs via the PCN-1 interface, will get the resources needed for the user mission.

This provisioning requires management of the services provided by the bearer networks through SLAs describing the services provided (Who gets and who provides the bearer Service? What are the characteristics of the provided bearer Service (VPLS, VPWS)? What are the Key Parameters describing the Service? What are the Quality Indicators relative to the service?).

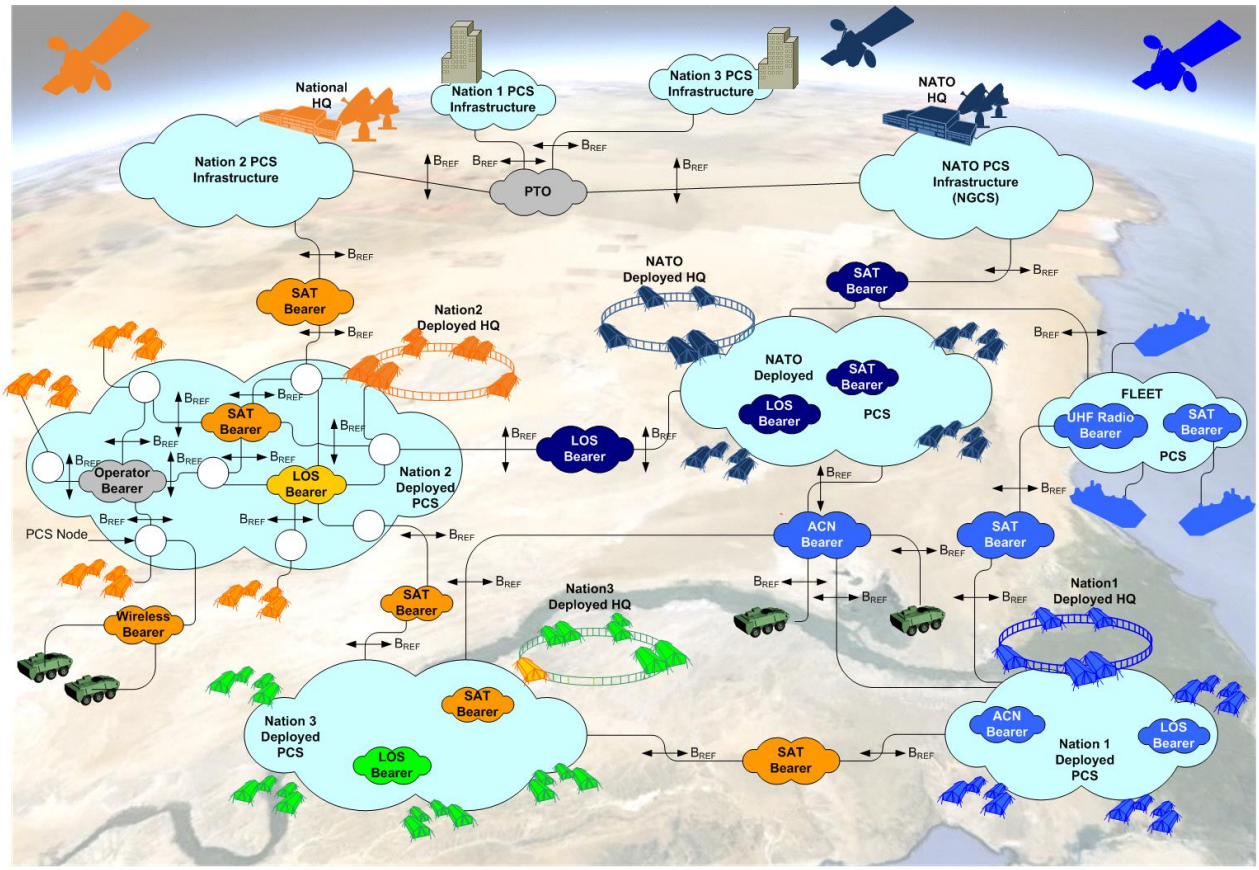

Figure 2 - System View showing the Bearer Networks

The previous figure is a system view that shows how the capacity is provisioned in order to answer to the capacity needs shown on the Operational view.

This second figure doesn't show the topology of the interconnection of PCSs nodes inside a PCS, and doesn't show the topology of the interconnection of the PCSs integrated in the same protected core network (PCore).

The topologies carried by the bearer sub-networks are illustrated on the following figure that shows:

- The PCN-1 Interfaces represented in blue
- The PCN-2 interfaces represented in green
- The interfaces inside a PCS (for PCS Nodes Interconnection) in Lavender. In order to lighten the figure, the interconnection between PCS Nodes is only illustrated for the Deployed Nation 2. These interconnections are presented as point to point trunks on the figure; with VPLS the figure would show point to multipoint interconnection capabilities.

The combination of the SLA specified for the B_{REF} Interface with the SLA specified for the PCN-1 or PCN-2 interfaces will specify as a whole the capabilities provided by the bearer network, and the way these capabilities are used for interoperability between PCSs (PCN-1) or for connection of mobile users to a PCS (PCN-2). The figure illustrates that a same B_{REF} Interface could be used as bearer of PCN-1 and PCN-2 interfaces.

Based on the $B_{REF,}$ PCN-1 and PCN-2 service description, the solution will provide the capability to specify any kind of interface, without any need to define service interoperability points according to the type of bearer network.

The services provided by the PCN-1 interfaces need to be provisioned and specified in and SLA, in order to make sure that the Protected Core Segments (PCSs) will get the resources required for their interoperability. The technical parameters specified in the PCN-1 SLA will be enforced by the adjacent PCSs.

The services provided by the PCN-2 interfaces need to be provisioned and specified in and SLA, in order to make sure that the Coloured Clouds hosted in the HQs, in the DOBs, or connected remotely will get the resources required for their mission. The technical parameters specified in the PCN-2 SLA will be enforced by the PCSs and shall also be enforced by the Coloured Cloud.

This provisioning requires management of the services provided by the PCSs through SLAs describing the services provided (Who gets and who provides the Service? What are the characteristics of the provided Service (Routing, Addressing, Security, etc)? What are the Key Parameters describing the Service? What are the Quality Indicators relative to the service?).

On the following figure the B_{REF} Interfaces have been removed and only the Trunk, PCN-1 and PCN-2 interfaces are represented. These interfaces are multiplexed on the B_{REF} Interface, and show the topology of the networks.

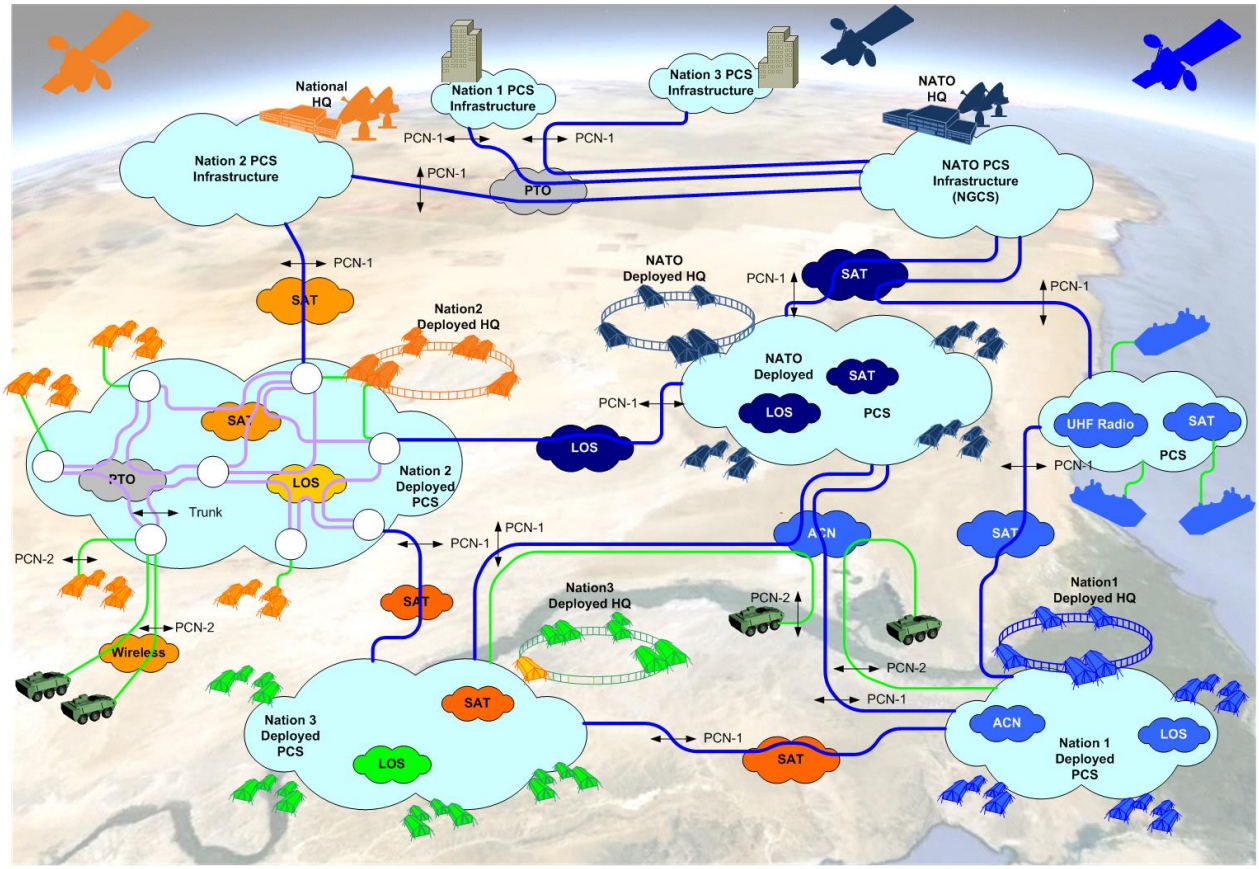

Figure 3 - System View - Topologies

IMPACT OF THE CONCEPTS ON THE SERVICE VALUE CHAIN

The system views developed in the previous chapter, clearly points out two levels in the architecture: the Bearer Sub-Networks in charge to provide the capacity, and the PCN level in charge to provide the connectivity to the HQs and DOBs for the operation.

The deployed Operational Bases and the Head Quarters shown on the figures host the coloured clouds (CCs). CCs are responsible for ensuring information confidentiality with their correspondent security domains, and must therefore apply confidentiality protection measures before sending information to the destination CCs through the PCN. This means that the PCN is A-Confidential (doesn't take into account any measure for confidentiality) and that the security measures integrated in the PCN are dedicated to Integrity and Availability.

In each security domain the CCs need to re-establish the IP connectivity and the QoS based on the connectivity and QoS provided by IP Crypto connected to the PCN, in order to be able to provide the adequate level of Service to the Information Systems hosted by the CC. The end-user services available in a CC are Multimedia Services (Web browsing, database browsing, messaging, chatting, video-conferencing, and telephony). These services may be provided by the same IS, but may also be provided by dedicated IS (Telephony, Data, Storage, etc) according to the size of the Coloured Cloud.

The following figure shows at high-level the Security and Service Value Chain.

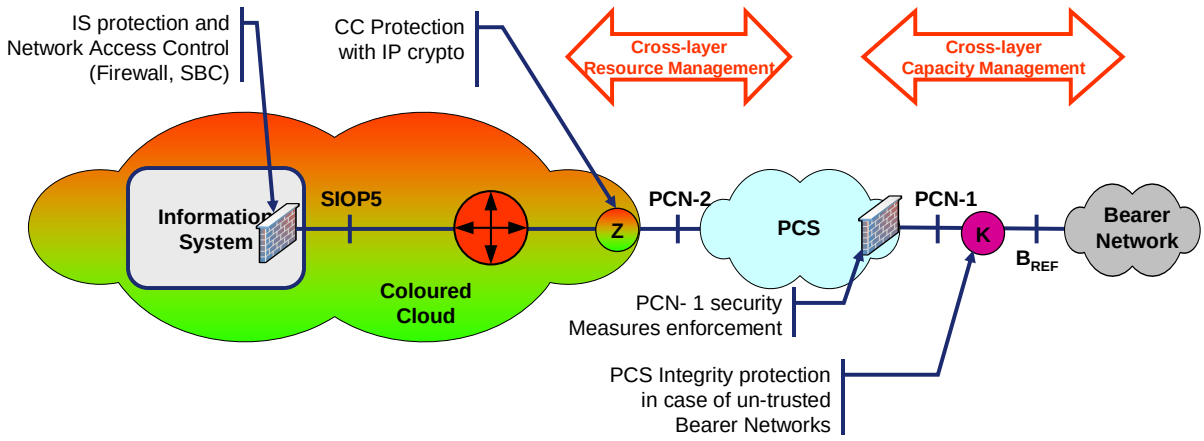

Figure 4 - Security and Service value chain

The security value chain is composed of following elements:

- The protection of the frames sent over the Bearer Networks. This protection is needed when the Bearer Network doesn't integrate any protection measure, or when it cannot be trusted. The objective of this protection is to avoid "passive listening, and intrusion in the routing and signalling protocols of the PCS". Such protection is needed in order to guarantee the Integrity and Availability of the Protected Core. In case of trusted bearer networks (ex: EPM satellite modem) this protection is not necessary.
- The enforcements of the security measures agreed in the SLA describing the PCN-1 interface. These security measures rely on filtering capabilities and network level intrusion detection.
- The IP Crypto required for the protection of each Coloured Cloud

- The protection mechanisms implemented in the Information System hosted in the CCs. According to the type of IS to protect, these mechanisms are based on Firewalls, and Session Border Controllers (SBC). These devices will also take into account the control functionalities dedicated to network access (authorised protocols, connection admission control, etc).

The Service Value Chain is composed of following layer implemented by following interfaces:

- The B_{REF} Interface that provides the capacity (bandwidth, range, etc) used by the PCSs for interconnection of its nodes and for interconnection with adjacent PCSs
- The PCN-1 Interface that provides interoperability with adjacent PCSs, this interface as indicated above is controlled with a service level description
- The PCN-2 Interface that provides the IP services to the Coloured Clouds, like the PCN-1 interface this interface is controlled with a service level description
- The SIOP5 Interface That provides the IP services inside the CCs to the Information Systems. The SIOP5 interface has been identified in the NNEC Feasibility study; this interface is controlled with a service level description.

Each of these networking layers will rely on services provided by the underlying layer in order to provide the services to be delivered either to upper networking layers or to the end-users. The policies specified in these Service Level Descriptions are enforced by the entities providing the service and by the entities using the service.

So, the services provided by the bearer networks are used for transport of PCN-1, PCN-2 and trunks, with the objective to provide the PCN-2 Service used by the coloured clouds. In the same way the coloured clouds use the service provided by the PCN-2 interface in order to provide the SIOP5 Service, which is used by the Information System for end-user Service provisioning.

Based on the Framework that is represented in Figure 4, the main issues that need to be solved are following:

- Cross-layer capacity management is needed, in order to allow the bearer network to indicate that the capacity provided by the interface has changed (dropped or increased). Such capacity changes will appear due to jamming environment or due to meteorological conditions (rain, snow, etc).

  These changes need to be reported to the PCS Nodes via standard protocols (ELMI or OAM flows), so that the PCS Node can re-configure the Scheduling mechanisms, the Reservation mechanisms, and the Routing protocols.
- Cross layer Resource Management is needed in order to allow the coloured clouds to request guaranteed resources for sessions setup dynamically. Such requests, sent by the CCs, will carry a precedence level that will be used by the PCS for pre-emption management on low capacity interfaces. There is a clear need for definition of Multi-Level Precedence and Pre-emption capabilities over PCN-1 interfaces, which will be carried over low capacity bearer networks.
- Service Level Management is in charge of a consistent provisioning of resources for the networking layers according to the final objectives of the mission. This networking architecture is considered as Service Oriented, because each networking layer will provide through the value chain capabilities exploited by higher levels.

POLICIES FOR PCS/PCN IMPLEMENTATION

Implementation of the PCN concepts will require further developments of policies that will be applied to the PCN-1, PCN-2, and B_{REF} interfaces. These policies shall determine a shared behaviour and common

understanding of the user and interoperability services provided by the PCN. The following list is not exhaustive but highlights what need to be addressed:

- The security policies applied to the PCSs integrated in a PCore need to be clarified with the objective to provide homogeneous requirements for the implementation, these requirements need to take into account the cross-layer issues presented in the previous paragraph.
- The QoS policy, based on the QENI development, need to be enhanced in order to take into account the requests for guaranteed resources dedicated to sessions, setup dynamically.
- In the PCN, forwarding will be based on IPV6, the routing and addressing policies should precise the addressing plan and the routing protocols that should be implemented on the PCN-1 interfaces (Static Routing, eBGP, Policy Based Routing). These policies should also highlight the constraints applying to the routing protocols implemented in the PCSs.
- Policies should also be developed in order to clarify the SLA templates describing the PCN-1, PCN-2, and B_{REF} interfaces. Such policies would ease the development of management solutions for the PCSs, and would ease the collaboration between the management systems of different PCSs.
- The management complements integrated in each PCS Network Operation Centre should be clarified in order to implement a minimum set of functions dedicated to collaboration inside the PCN and to hypervision of the PCN.

CONCLUSION

The application of the PCN concept to a coalition deployment shows that, according to the operational requirements, it is possible to plan the capacities and topologies that need to be deployed for interconnecting the deployed operational bases. The capacity will be provided by bearer sub-networks providing in a near future VPWS and a VPLS services, and the connectivity and quality of service will be provided by the PCN, which will manage the security constraints (Integrity and Availability). The PCN architecture should integrate in the architecture design the bearer sub-networks, in order to clarify the role of each networking component (Bearer, PCS).

The Security and Service value chain shows the services that need to be provisioned. The value chain shows the technical issues that have to be analysed (Layer 2 Encryption devices, QoS Cross-Layering, ELMI/OAM flow management, SLA management). Development of these issues will require clear policies be established between NATO and the Nations (Security, Routing, QoS, SLA Template, and Management).

Current deployment and architectures manage interoperability in interconnecting the Information Systems. The PCN concept doesn't solve all the interoperability issues, which need to be addressed for interconnection of Information Systems in the static domain, and in the coalition deployed domain. These interoperability capabilities require implementation of Information Exchange Gateways in the static domain, and implementation of Interface Modules and Gateways in the deployed domain. They are in charge to control the protocols and the information exchange allowed on the interfaces.

In the context of a deployment of a coalition, the PCN concept will provide the connectivity needed by these gateways, and allow minimisation of their quantity in the deployment. For example it is possible to consider that each nation only deploys one or two (for redundancy) Interface Modules interconnected through the PCN with the other Interface Modules deployed by NATO and by the other nations. So with the presented solution there is no need to interface these gateways locally with legacy protocols if all the services have converged to IP.

The PCN concept finds many early adopters making decision for early implementation of PCS concepts. These early implementations will be based on standard protocols (IP, Static Routing, eBGP, etc) and

standard policies like QENI, in order to be compliant with further improvements integrating Policy Based Routing, Load Balancing, Real Time Automatic Risk Assessment, Dynamic Accreditation, etc. They will also be based on layer 2 encryption capabilities dedicated to protection of the headers, the signalling and routing protocols. These layer 2 encryption devices will replace the Bulk Crypto devices and will have to provide Traffic Flow Confidentiality and Intrusion detection and avoidance.

This white paper shows that many networks will be PCN Compliant and will cooperate for the benefit of the operations, and for the benefit of NATO and of the nations. Further studies are required in order to analyse the visibility that each PCS gives to the PCores it belongs to.

From another point of view, a same Infrastructure Network could host several PCS dedicated to different missions, allocated each one with its own resources.

The PCN Concept finds early adopters, because this concept addresses:

- The services to be delivered to the Coloured Clouds (taking into account the quality of service and policies)
- The Interoperability between the networks deployed by the forces of a coalition. The PCN concept allows to reduce the amount of Interface Modules required for Service Interoperability
- The Flexibility needed for the deployments: Multiple PCSs in a PCN dedicated to one deployment, Mobility of the PCSs inside a same PCN,
- The footprint, which size needs to be as low as possible when deployed on a theatre of operation
- The basic security requirement of a network, and proposes a clear separation between Confidentiality that is managed in the Coloured Cloud, and Integrity and Availability that needs to be managed by the PCore.

This paper also shows that the PCN concept is compliant with the undergoing transformation of legacy bearer networks services (Vxx, PDH, SDH) to wide area advanced Ethernet Services (VPWS and VPLS).

REFERENCES

[NNEC]: NATO Network Enabled Capability Feasibility Study

[NCRA]: NATO Information Infrastructure Communication Reference Architecture

[SGRA]: NATO SATCOM Ground Reference Architecture

[QENI]: NATO QoS Enabled Network Infrastructure

[PCN]: Requirements for a Protected Core Networking (PCN) - Interoperability Specification (ISpec)